UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/447,500	11/23/1999	ROBERT DAVID GRAHAM	003845.P0001	3902

7590 09/30/2003

W. Scott Petty
KING & SPALDING
191 Peachtree Street
45th Floor
Atlanta, GA 30303-1763

EXAMINER	
VAUGHAN, MICHAEL R	
ART UNIT	PAPER NUMBER
2131	9

DATE MAILED: 09/30/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/447,500	Applicant(s) GRAHAM, ROBERT DAVID
	Examiner Michael R Vaughan	Art Unit 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-40 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-40 is/are rejected.

7)☒ Claim(s) 40 is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 23 November 1999 is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 2-4,7,8 .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

Detailed Action

Claims 1-40 have been examined and are pending.

Drawings

The drawings are objected to because: in figures 1-9 the lines, numbers, and letters are not uniformly thick and well define (see 37 CFR 1.84(i) and 37CFR 1.84(p) and accompanied Draftsperson's Review). A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Claim Objections

Claim 40 is objected to because of the following informalities: "pervious" should be –previous--. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Regarding claim 15, the phrase "e.g. (for example)" renders the claim indefinite because it is unclear whether the limitation(s) following the phrase are part of the claimed invention. See MPEP § 2173.05(d).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-3, 18-22, 24-28, 31, 32, 35, 36, 39, 40 are rejected under 35 U.S.C. 102(b) as being anticipated by Johnson et al (USP 5,345,595).

As per claim 1, Johnson et al teach:

modifying an alert variable based on data transmissions originating from one or more suspects nodes (column 3, lines 5-25);

triggering a first response when said alert variable reaches a first predetermined threshold level (column 3, lines 14-25);

triggering a second response when said alert variable reaches a second predetermined threshold level (column 3, lines 25-40).

As per claim 2, Johnson et al teach triggering additional responses when said alert variable reaches one or more additional threshold levels (column 6, line 61 – column 7, line 20).

As per claim 3, Johnson et al teach passive scanning (looking) of one or more of said suspect nodes (column 3, lines 57-61).

As per claim 18, Johnson et al teach:

modifying a first suspect-specific alert variable (each call pattern event) based on data transmissions originating from a first suspect node (column 9 and column 10, lines 3-44);

modifying a second suspect-specific alert variable (each call pattern event) based on data transmissions originating from a second suspect node (column 9 and column 10, lines 3-44);

triggering a suspect-specific response when either of said suspect-specific alert variables reach a predetermined threshold level (column 4, lines 16-26).

As per claim 19, Johnson et al teach triggering additional suspect-specific responses when either of said suspect-specific alert variables reaches additional predetermined threshold values (column 6, line 61 – column 7, line 20).

As per claim 20, Johnson et al teach modifying an overall alert variable based on said data transmissions originating from each suspect node (column 9 and column 10, lines 3-44).

As per claim 21, Johnson et al teach triggering a response towards each one of said plurality of suspect nodes when said overall alert variable reaches a predetermined threshold value (column 6, line 61 – column 7, line 20).

As per claim 22, Johnson et al teach the alert variable is more responsive to new types of data transmissions than to data transmissions previously received at said network node (column 6, line 61 – column 7, line 20).

As per claim 24, Johnson et al teach communicating each of said suspect-specific alert variables to a network database residing on a server node (column 6, lines 61-65).

As per claim 25, Johnson et al teach communicating said overall alert variable to a network database residing on a server node (column 6, line 61 – column 7, line 20).

As per claim 26, Johnson et al teach:

storing a plurality of suspect-specific alert variables for a plurality of network nodes (column 6, lines 61-65);

modifying a network alert variable based on the value of each of said plurality of suspect-specific alert variables (column 9 and column 10, lines 3-44);

triggering a network response when said network alert variable reaches a predetermined threshold level (column 4, lines 16-26).

As per claim 27, Johnson et al teach notifying each of the plurality of network nodes (system operators) that they should each increase their suspect-specific alert variable (alert-state) towards a particular suspect node.

As per claim 28, Johnson et al teach a network server node initiating a passive scan of a particular suspect node (column 24, lines 30- 40). The suspect node is monitored (passively) for a window of time.

As per claim 31, Johnson et al teach:

storing a plurality of overall alert variables for a plurality of network nodes (column 9, lines 29-43 and column 21, lines 27-50);

modifying a network alert variable based on the value of each of said plurality of overall alert variables (column 9 and column 10, lines 3-44);

triggering a network response when said network alert variable reaches a predetermined threshold level (column 4, lines 24-26 and FIG. 4C block S540).

As per claim 32, Johnson et al teach:

receiving a first event from a suspect node (column 3, lines 14-25);

recording said first event in a first data structure having an event count value (column 6, lines 61-65 and column 9, lines 11-18);

receiving a second event from said suspect node, said second event (new event) being of a same type as said first event (column 6, line 61 – column 7, line 20);

recording said second event in said first data structure(column 6, lines 61 – column 7, line 5) and incrementing a said count value (call events are counted and numbered (column 16, lines 62-64)) if said second event occurs within a predetermined window of time after said first event (column 22, 1-20). Johnson et al teach that the window of time is different depending on the event. The data of the database event is compared to the call date.

As per claims 35 and 36, Johnson et al teach the event type influences the predetermined window of time (column 21, line 27 – column 22, line 22). A simultaneous call event would have a window time of the duration of the call. However, a "Double Duration" event (column 24, lines 8-36) has a window time of four to five days. Johnson et al teach that there are two levels of alert, yellow and red (column 30 lines 2-6). The window time for a red alert such as "Double Duration" is up to five days, which is more than the window time for a yellow alert.

As per claim 39, Johnson et al teach generating a report of all new events, which occur over a predetermined time period (column 6, lines 61 – column 7, line 16 and column 21, lines 26-50).

As per claim 40, Johnson et al teach:

determining whether said event is included in a single data structure with one or more previous events received in a time period preceding said predetermined time period (column 6, lines 61-68 and column 21, lines 12-19);

searching all data structures generated during said time period preceding said predetermined time period if said event is not included in said single data structure with one or more previous event (column 6, lines 61 – column 7, line 16).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

-7, 10-14, 16-17, 23, 25-30, 33-34 and 37

Claims 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Johnson et al in view of Hershey et al (USP 5,414,833).

As per claim 4, Johnson et al teach passively scanning a node. Johnson et al are silent in disclosing the step of recording data transmissions in a log file (column 2, lines 41-42). Hershey et al teach a conventional method of storing data in a log file. In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teaching of Hershey et al within the system of Johnson because it would allow the passively scan data to be recorded to a log file where it could be later analyzed.

As per claim 5, Johnson et al are silent in disclosing the triggered responses that include an active scan of suspected nodes. Hershey et al teach actively scanning suspected nodes (column 9, lines 24-26). Hershey et al teach that an adaptive active responding means provide the functionality necessary to implement a security agent in a high-speed communication environment (column 9, lines 34-38). In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teaching of Hershey et al within the system of Johnson et al because it would allow the system to have greater control and responsiveness to a node suspected of misconduct.

As per claim 6 and 7, Johnson et al are silent in disclosing an active scan which includes the step of retrieving information about one or more suspect nodes including the network address of said suspect

nodes. Hershey et al teach a security agent which can gather information such as viral detection (column 7, 3-6), inappropriate use (column 7, lines 7-15), and detect logins (column 7, lines 16-19) about a suspected node. The security agent monitors the bits on the network and can detect protocol information (column 9, lines 40-50). If a security agent knows the protocol information a node in the network, it then knows the network address of all nodes and the route in which the suspected node's data travels. In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teaching of Hershey et al within the system of Johnson because it would allow the security system to retrieve information about a suspected node and know where it is transmitting.

As per claim 10, Johnson et al are silent in disclosing the step of blocking incoming data transmissions. Hershey et al discloses that a device could delete information in the bit stream. Deleting the bit stream in synonymous to blocking the bits from reaching their destination. The ability to block the bits from reaching their destination is an important active security feature. In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teaching of Hershey et al within the system of Johnson because it would allow the system to have active control over the transmitting of data within the network.

As per claim 11, Johnson et al are silent in disclosing that an alert variable responds differently over time to a particular type of data transmission. Hershey et al disclose that bit pattern detection can be actively changed to recognize new bit pattern on the network (column 11, line 60 – column 12, line 12). This means that over time, when new viruses for instance are discovered, the system can be adapted to detect the new bit patterns. In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teaching of Hershey et al within the system of Johnson because it would allow the system to be adaptable so that it can detect bit patterns which are found in the future to be dangerous to the network (worms).

As per claim 12, Johnson et al teach that the numbers of calls (data transmission) are counted until a threshold is reached (column 3, lines 14-25).

As per claim 13, Johnson et al are silent in disclosing that a particular type of data transmission originating from a said suspect node is an invalid login attempt. Hershey et al teach that invalid login

attempts are monitored to provide the network security from intruders who are trying to guess login combinations (column 22, lines 36-61). In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teaching of Hershey et al within the system of Johnson because it would allow the system to prevent authorized users from gaining access to the system by trying to match login names with passwords.

As per claim 14, Johnson et al teach that a moving average adapts to the user's data transmission patterns (column 9 – column 10). Johnson et al teach that a decision to create an alert is made by comparing some event to a threshold level (column 9, lines 5-14). Averaging events over a time period smoothes out a user's data and thereby create a trend (column 10, lines 9-10). At first the data would be erratic and send frequent alerts but as the trend is defined the system becomes less sensitive (higher threshold) to a day with more than usual data transmission. Therefore it is inherent that Johnson et al teaches a system whereby at first, changes in a user's trend create alerts but if they are continued the system adapts to the new level of use and does not report false alerts.

As per claims 16 and 17, Johnson et al are silent in disclosing filtering data on the packet level. Hershey et al teach a security system that can be implement on the TCP/IP level of the network stack (column 31, line 61- column 33, line 10). Hershey et al teach network protocol information is decipherable at the IP level the important. It is therefore inherent that from the teaching of Hershey et al, the system can be implemented on the IP level to analyze and filter data packets. Hershey teaches the gathering of network information from protocol data (column 9, lines 40-50). In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teaching of Hershey et al within the system of Johnson because it would allow the system to analyze and filter data at the packet level where network protocol overhead can be easily discerned and used to expedite security actions.

As per claim 23, Johnson et al teach that a moving average adapts to the user's data transmission patterns (column 9 – column 10). Johnson et al teach that a decision to create an alert is made by comparing some event to a threshold level (column 9, lines 5-14). Averaging events over a time period smoothes out a user's data and thereby create a trend (column 10, lines 9-10). At first the data

would be erratic and send frequent alerts but as the trend is defined the system becomes less sensitive (higher threshold) to a day with more than usual data transmission. Therefore it is inherent that Johnson et al teaches a system whereby at first, changes in a user's trend create alerts but if they are continued the system adapts to the new level of use and does not report false alerts.

As per claim 29, Johnson et al are silent in disclosing the triggered responses that include an active scan of suspected nodes. Hershey et al teach actively scanning suspected nodes (column 9, lines 24-26). Hershey et al teach that an adaptive active responding means provide the functionality necessary to implement a security agent in a high-speed communication environment (column 9, lines 34-38). In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teaching of Hershey et al within the system of Johnson because it would allow the system to have greater control and responsiveness to a node suspected of misconduct.

As per claim 30, Johnson et al are silent in disclosing the step of blocking incoming data transmissions. Hershey et al discloses that a device could delete information in the bit stream. Deleting the bit stream in synonymous to blocking the bits from reaching their destination. The ability to block the bits from reaching their destination is an important active security feature. In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teaching of Hershey et al within the system of Johnson because it would allow the system to have active control over the transmitting of data within the network.

As per claim 33, Johnson et al teach that alerts are recorded in a data structure (column 6, lines 61-63). Johnson et al teach that from the records of events, the data (CCF record) is used to adjust the moving average of use to form a pattern (column 10, lines 3-15). The data is used to formulate the user trend whether it falls within the window of time or not. If only the data from inside the window of time was used to formulate the average, the result would not depict an accurate picture of a user's trend. The data outside the window of time must also be incorporated to calculate an accurate average of network use. Therefore it is inherent that the teachings of Johnson et al suggest events that occur outside the window of time (those that do not cause an immediate alert) are also recorded and used to generate an average.

As per claim 34, Johnson et al teach that a moving average adapts to the user's data transmission patterns (column 9 – column 10). Johnson et al teach that a decision to create an alert is made by comparing some event to a threshold level (column 9, lines 5-14). Averaging events over a time period smoothes out a user's data and thereby create a trend (column 10, lines 9-10). Thus the window of time is changed with events that occur. For example the window of time would gradually increase if the user started making more calls each day (increased data). At first the data would be erratic and send frequent alerts but as the trend is defined the system becomes less sensitive (higher threshold) to a day with more than usual data transmission. Therefore it is inherent that Johnson et al teaches a system whereby at first, changes in a user's trend create alerts but if they are continued the system adapts by adjusting the window of time so that the system does not report false alerts.

As per claim 37, Johnson et al are silent in disclosing that a particular type of data transmission originating from a said suspect node is an invalid login attempt. Hershey et al teach that invalid login attempts are monitored to provide the network security from intruders who are guessing to guess login combinations (column 22, lines 36-61). In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teaching of Hershey et al within the system of Johnson because it would allow the system to prevent authorized users from gaining access to the system by trying to match login names with passwords.

Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Johnson et al in view of Watson et al (USP 5,475,839).

As per claim 8, Johnson teaches responding to triggered network events (column 3, lines 14-25). Johnson et al are silent in disclosing that in authentication if increased in order to gain access to the network resources. Watson et al teach that once an invalid login is detected that the user has a certain number of chances to login correctly before the system is shut down (column 14, lines 11-33). Watson et al also teach that the computer will shut itself down each time a login fails. The user must then login successfully on the first try in order to return the computer back its default state. Therefore the authentication is increased once a suspicious event has been detected. In view of this it would have

been obvious to one of ordinary skill in the art at the time of the invention to employ the teaching of Watson et al within the system of Johnson et al because it would allow the system to respond to security threats by enforcing and passing a stronger authentication process in order to gain access to the network resources.

Claim 38 is rejected under 35 U.S.C. 103(a) as being unpatentable over Johnson et al in view of "Packages in the net directory" (note that this reference will be referred to as Packages hereafter).

As per claim 38, Johnson et al are silent in disclosing a ping event type. Packages teach a tool known as tcpdump, which can be used to detect ping attacks and monitor the network (pg. 14). Ping attacks are a network problem, as Packages teach, because they can slow-down the system or a target node by flooding it with packets. In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teaching of Packages within the system of Johnson et al because it would allow the system to recognize ping packets and determine if they are a threat to the system.

Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Johnson et al and Watson et al as applied to claims 1 and 8 above, and further in view of CamNet (Using the CamNet BBS FAQ).

As per claim 9, the combined teachings of Johnson et al and Watson et al teach increasing the authentication of the system when an invalid login occurs. The combined teachings of Johnson et al and Watson et al fail to teach requiring the user to login twice in order to gain access to the network resources. Having a login twice increases the security and decreases the chance of an authorized user from gaining access to the network. CamNet teaches requiring a user to login twice in order to gain full access to the system (pg. 1). In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teaching of CamNet within the combined system of Johnson et al and Watson et al because it would require a user to login twice in order to gain access to the network resources.

Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Johnson et al and Hershey et al as applied to claims 1, 11, and 14 above, and further in view of NASIRE (NASA Automated Systems Incident Response Capability).

As per claim 15, the combined teachings of Hershey et al and Watson et al fail to teach a particular type of data transmission originating from said suspect node is a transmission that retrieves information about said network. NASIRE teaches that sniffer programs compromise a network by subjecting itself to all data (information) on the network (pg. 1). By doing so it can obtain any information being sent on the network. NASIRE teaches that these program need to be detected so that they can be shut down. In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teaching of NASIRE within the combined system of Johnson et al and Hershey et al because it would increase the overall security of the network by detecting nodes which are using programs or techniques that compromise the resources of the network by gaining unauthorized information.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Accessing the ESOS through the Network, see reference sheet for bibliographic information.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael R Vaughan whose telephone number is 703-305-0354. The examiner can normally be reached on M-F 7-3:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

MV
Michael R Vaughan
Examiner
Art Unit 2131

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100